

Amendments to the Abstract:

Please delete the Abstract of the Disclosure in its entirety and substitute the following replacement Abstract therefor:

ABSTRACT OF THE DISCLOSURE

In a method for protected execution of a cryptographic calculation in which a key with at least two key parameters is drawn on, an integrity check of the key is performed, in order to prevent a cryptographic attack in which conclusions are drawn as to at least one second key parameter by corrupting at least one first key parameter. A further method serves to determine a key for a cryptographic calculation with at least two key parameters provided for use in the first-mentioned method. A computer program product and a portable data carrier have corresponding features. The methods enable particularly good protection of cryptographic calculations against attacks.